CLAIMS

1. A method for assessing a vulnerability in an image having a file and a configuration setting, comprising:

providing access to the image to allow the configuration setting to be manipulated;

identifying the vulnerability in the image; and

eliminating the vulnerability in the image by manipulating the configuration setting or file.

2. A method for assessing a vulnerability in an image as recited in claim 1 wherein providing access to the image to allow the configuration setting to be manipulated further includes providing access to the file and the configuration setting.

3. A method for assessing a vulnerability in an image as recited in claim 1 wherein eliminating the vulnerability in the image by further includes updating the configuration setting.

4. A method for assessing a vulnerability in an image as recited in claim 1 wherein eliminating the vulnerability in the image further includes modifying the file.

5. A method for repairing an image comprising:

scanning the image;

detecting a vulnerability in an image;

determining a definition configured to repair the vulnerability in the image; and

repairing the image using the definition as though the image was an independent system.

6. A method for repairing an image as recited in claim 5 wherein the definition includes a corrective measure.

7. A method for repairing an image as recited in claim 5 wherein determining the definition further includes testing the definition before applying the definition to the image.

8. A method for repairing an image as recited in claim 5 further including determining whether the vulnerability affects the configuration setting.

9. A method for repairing an image as recited in claim 5 further including determining the location of the vulnerability.

10. A method for repairing an image as recited in claim 5 wherein the image has a configuration setting and further including implementing the definition in the configuration setting.

11. A method for repairing an image as recited in claim 5 further including implementing the definition in a file associated with the image.

12. A method for repairing an image as recited in claim 5 wherein detecting a vulnerability in an image further includes evaluating an image of a machine, the machine configured to run as a system.

13. A method for repairing an image as recited in claim 5 wherein detecting a vulnerability in an image further includes abstracting a physical resource of the system to generate a virtual machine, the virtual machine representing a collection of resources to execute an application.

14. A method for repairing an image as recited in claim 5 wherein determining a definition configured to repair the vulnerability in the image further includes comparing the definition to the image to yield a result whereby the result indicates whether the definition is current.

15. A method for repairing an image as recited in claim 5 wherein determining a definition configured to repair the vulnerability in the image further includes comparing the definition to a criterion to determine whether to apply the definition to the image.

16. A method for repairing an image as recited in claim 5 wherein determining a definition configured to repair the vulnerability in the image further includes verifying a key in a registry associated with the image.

17. A method for repairing an image as recited in claim 5 wherein determining a definition configured to repair the vulnerability in the image further includes scanning a storage associated with the image.

18. A method for repairing an image as recited in claim 5 wherein determining a definition configured to repair the vulnerability in the image further includes scanning a processor state associated with the image.

19. A method for repairing an image as recited in claim 5 wherein determining a definition configured to repair the vulnerability in the image further includes modifying a storage associated with the image.

20. A method for repairing an image as recited in claim 5 wherein determining a definition configured to repair the vulnerability in the image further includes modifying a processor state associated with the image.

21. A system for securing an image comprising:

an engine configured to detect a vulnerability in an image having a configuration setting;

a logic module configured to determine a definition configured to secure the image and to test the definition before applying the definition to the image; and

an access module for restoring the image using the definition.

22. A system for securing an image as recited in claim 17 wherein the engine further includes a decomposer configured to abstract the image of a machine.

23. A system for assessing a vulnerability in an image comprising:

a logic for assessing a vulnerability in an image;

a virtualization module for abstracted the image from a file; and

a decomposer for writing data to a registry.

24. A data signal embodied in a carrier wave comprising:

instructions for detecting a vulnerability in an image having a configuration setting;

instructions for determining a definition configured to secure the image;

instructions for testing the definition before applying the definition to the image; and

instructions for restoring the image using the definition.

25. A computer program product for assessing a vulnerability in an image, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

detecting a vulnerability in an image having a configuration setting;

determining a definition configured to secure the image;

testing the definition before applying the definition to the image; and

restoring the image using the definition.